VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

SEMESTRÁLNÍ PRÁCE

Brno, 2019 Bc. Juraj Korček

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

APLIKACE PRO GENEROVÁNÍ A OVĚŘOVÁNÍ KONFIGURACÍ SÍŤOVÝCH ZAŘÍZENÍ
APPLICATION GENERATING AND VERIFYING CONFIGURATIONS OF NETWORK DEVICES

SEMESTRÁLNÍ PRÁCE
SEMESTRAL THESIS

AUTOR PRÁCE — **Bc. Juraj Korček**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Jan Jeřábek, Ph.D.**
SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Semestrální práce

magisterský navazující studijní obor **Informační bezpečnost**
Ústav telekomunikací

Student: Bc. Juraj Korček ***ID:*** 187238
Ročník: 2 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Aplikace pro generování a ověřování konfigurací síťových zařízení

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s problematikou síťových zařízení, síťových operačních systémů, hlavních používaných komunikačních protokolů a způsobů konfigurace těchto zařízení. Dále prostudujte problematiku osvědčených postupů konfigurace, zejména s ohledem na bezpečnost fungování zařízení v síti a také problematiku anonymizace těchto konfigurací. Navrhněte systém či aplikaci, která bude umět pro vybranou množinu síťových zařízení vytvářet přednastavené parametry nastavení, které bude možné na dané síťové zařízení aplikovat. Dále musí daná aplikace umět verifikovat správnost existujících konfigurací, upozornit na případné nedostatky a i konfiguraci modifikovat tak, aby splňovala hlavní bezpečnostní a provozní standardy a doporučení. Fungování aplikace ověřte na testovacích vzorcích síťových konfigurací různých zařízení z několika různých sítí a případně i různých výrobců.
V rámci semestrálního projektu je třeba vypracovat teoretickou část zadání, vybrat vhodné programovací prostředí pro plánovanou aplikaci a navrhnout a popsat strukturu dané aplikace či systému, včetně základního popisu jednotlivých komponent a jejich předpokládané funkcionality. Vlastní řešení mírně rozpracujte.

DOPORUČENÁ LITERATURA:

[1] Stallings W., Network security essentials: applications and standards. 6th ed. Hoboken: Pearson education, 2017, 445 s. ISBN 978-0-13-452733-8.

[2] McMillan, T., CCNA Security Study Guide: Exam 210-260. 2nd ed. USA: Sybex, 2018, 384 s. ISBN 978-1--1-940993-9.

Termín zadání: 23.9.2019 ***Termín odevzdání:*** 21.12.2019

Vedoucí práce: doc. Ing. Jan Jeřábek, Ph.D.
Konzultant:

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

VYHLÁSENIE

Vyhlasujem, že svoju semestrálnú prácu na tému „Aplikace pro generování a ověřování konfigurací síťových zařízení“ som vypracoval samostatne pod vedením vedúceho semestrálnej práce, s využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej semestrálnej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto semestrálnej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autora

Obsah

Zoznam obrázkov

Zoznam tabuliek

Zoznam výpisov

Úvod

Kybernetická bezpečnosť je bezpochyby jednou z hlavných tém 21. storočia. Útoky na infraštruktúru a systémy naberajú nielen na frekvencii, ale čo je ešte horšie na sofistikovanosti. Napriek častému zdôrazňovaniu odborníkov o kladenie čoraz väčšieho dôrazu na bezpečnosť pri návrhu, implementácii a nasadeniu, sa stále stretávame s fatálnymi dôsledkami, ktoré boli spôsobené nedostatočným venovaním pozornosti bezpečnosti.

Problém nedostatočného zabezpečenia nie je ani tak nevedomosť základných bezpečnostných praktík administrátorov alebo programátorov, ale potreba rýchleho nasadenia systému a infraštruktúry s odložením implementácie bezpečnostných praktík na neskôr. Tieto problémy vznikajú aj pri dodatočnej implementácií nových modulov a pridaní novej infraštruktúry, kedy sa nemení celok, ale pridanie jednej časti môže výrazne ovplyvniť a zmeniť stav bezpečnosti celého systému. Z tohto dôvodu je priam žiadúce disponovať nejakým procesom alebo nástrojom na dodatočné zistenie nedostatkov a ich následnú elimináciu. Veľmi silnou motiváciou by malo byť aj to, že dôsledkom bezpečnostných nedostatkov sú globálne miliardové škody a straty reputácií firiem.

Jednou z hlavných častí infraštruktúry, kde dochádza k významným bezpečnostným incidentom je počítačová sieť, bez ktorej by dnes informačné technológie nevedeli fungovať. Preto sa táto práca bude zaoberať práve ňou, keďže je vstupnou bránou do systémov a jej vyradením alebo zneužitím prichádzajú organizácie o finančné prostriedky, citlivé dáta a dôveru užívateľov.

Výsledkom tejto práce bude aplikácia overujúca nastavenia sieťových zariadení prevažne v lokálnej sieti, ktorá umožňuje zjednať nápravu na základe nájdených nedostatkov. Výhodou oproti existujúcim riešeniam bude otvorenosť kódu a modularita, ktorá umožní rozšírenie aplikácie na sieťové zariadenia rôznych výrobcov. Dôležitým výstupom bude taktiež zoznam bezpečnostných a prevádzkových odporučaní vychádzajúcich z rôznych štandardov a odporučaní, ktoré môžu byť v budúcnosti použité ďalšími užívateľmi aplikácie pri zostavovaní modulov pre zariadenia rôznych výrobcov. Jednou z kľúčových vlastností je bezplatnosť, keďže podľa zistení takmer polovica útokov smeruje na malé firmy, ktoré bezpečnosť často neriešia z finančnej náročnosti programov na detekciu bezpečnostných nedostatkov.

1 Kybernetická bezpečnosť

S čoraz na väčšou informatizáciou naprieč všetkými odvetviami života, je nutnosťou riešiť aj zabezpečenie systémov, infraštruktúry a dát. Kybernetická bezpečnosť je bez pochýb jednou z najdiskutovanejších tém 21. storočia.

Podľa zistení z roku 2018 takmer polovica útokov smeruje na malé firmy, ktoré bezpečnosť riešia iba minimálne alebo vôbec. Predpokladá sa, že pre rok 2019 bude na kybernetickú bezpečnosť minutých 6 miliárd dolárov, naopak škody spôsobené kybernetickými útokmi presiahnu jednu miliardu dolárov a veľmi záškodné útoky typu *Distributed Denial of Service – distribuované odoprenie služby* (DDoS) by mali vzrásť až šesťnásobne. [1]

Vyššie zmienené predpovede len potvrdzujú dôležitosť kybernetickej bezpečnosti pri návrhu, implementácie, nasadzovaní a prevádzke informačných technológií.

1.1 Vybrané pojmy z kybernetickej bezpečnosti

- Informačné aktívum (Asset) – čokolvek, čo je nutné chránit, napr. dáta, fyzická informačná infraštruktúra, systémy [3].

- Zraniteľnosť (Vulnerability) – neprítomnosť alebo nedostatočné opatrenia na zabezpečenie. Zraniteľnosť môže byť prítomná hardvéri, softvéri alebo samotnom užívateľovi [3].

- Hrozba (Threat) – vzniká v prípade odhalenia alebo zneužitia zraniteľnosti. Zároveň platí, že hrozbou je aj zraniteľnosť, ktorá doposiaľ nebola neidentifikovaná [3].

- Útočník (Threat agent) – entita, ktorá zneužije zraniteľnosť [3].

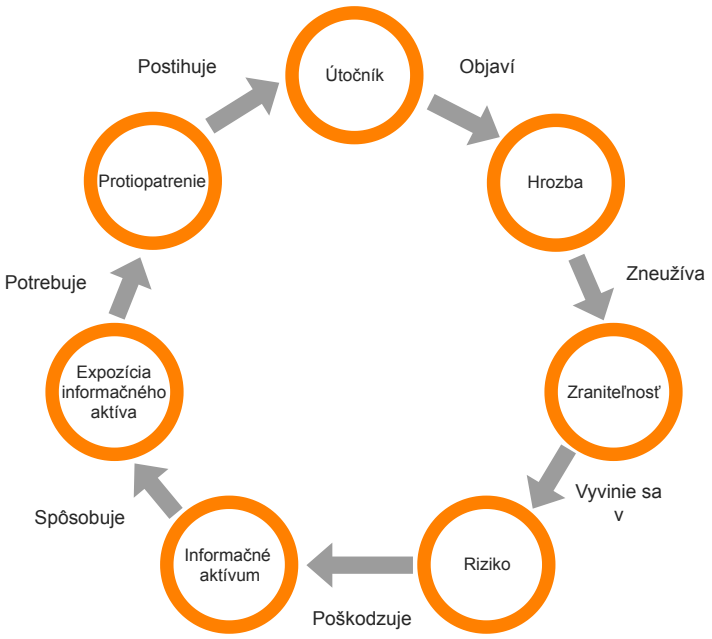
- Riziko (Risk) – pravdepodobnosť, že útočník využije zraniteľnosť, pričom príde k dopadu na systém alebo infraštruktúru [3].

- Útok na bezpečnosť (Security attack/Explotation) – krok, ktorý kompromituje bezpečnosť informačného aktíva [2].

- Bezpečnostný mechanizmus (Security mechanism) – proces, ktorý je navrhnutý na detegovanie, prevenciu a zotavenie z útoku na bezpečnosť.

- Protiopatrenie (Countermeasure) – ochranné opatrenie, ktoré znižuje riziko [3].

- Expozícia informačného aktíva (Exposure) – dochádza k nej ak je aktívum vystavené stratám nedostatočným alebo neprítomným zabezpečením [3].



Obr. 1.1: Koncept bezpečnosti a vzájomné vzťahy pojmov [3]

Na obrázku 1.1 je možné vidieť vzájomnú interakciu medzi pojmami. Zároveň je nutné si uvedomiť, že takýto cyklus nie je v systéme alebo infraštruktúre jeden a taktiež môže vzniknúť niekoľko paralelných cyklov pričom každý môže mať počiatok v inom uzle. Je dobré myslieť na to, že jednotlivé cykly môžu na seba vplývať, napríklad jedno protiopatrenie môže postihnúť viacero útočníkov využívajúcich rôzne hrozby.

1.2 Ciele sieťovej bezpečnosti

Bezpečnosť počítačovej siete, tak ako aj iných podoblastí kybernetickej bezpečnosti je založená na troch základných princípoch známych ako *confidentiality, integrity, availability – dôvernosť, integrita, dostupnosť* (CIA). Bezpečnosť musí pokryť všetky tri aspekty popísané týmto modelom, pričom narušenie čo i len jednej zložky má za následok nesplnenie celkového zabezpečenia [2].

1.2.1 Triáda CIA

- Confidentiality (Dôvernosť) – zabránenie prístupu k dátam alebo informáciám neoprávneným osobám. Na zaistenie tejto požiadavky sa najčastejšie používa šifrovanie, ale aj autentizácia a autorizácia. Jej strata vedie k neoprávnenému zverejnenie informácií. [3]
- Integrity (Integrita) – dáta alebo informácie sú zabezpečené proti neautorizovanej modifikácií a poškodeniu. Týmto zaisťujem konzistenciu dát pri prenose alebo uchovaní na médiu. Integritu zaisťujeme hašovacími funkciami prípadne za pomoci *Access Control List – zoznam pre riadenie prístupu* (ACL). [3]
- Availability (Dostupnosť) – dáta alebo informácie sú dostupné iba pre určité entity v daný čas a miesto. [3]

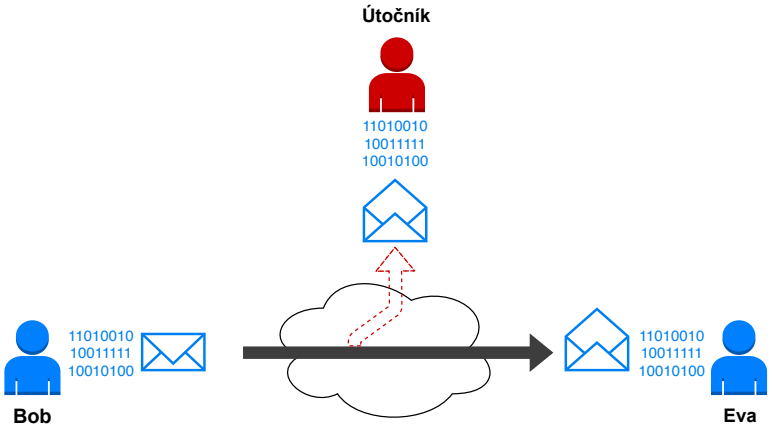
Obr. 1.2: Triáda dôvernosť, integrita a dostupnosť [2]

Aj keď triáda CIA definuje ciele na zaistenie bezpečnosti, tak niektorí odborníci ju nepovažujú za dostatočnú a zavádzajú ďalšie dve podmienky a pojmy:

- Authencity (Autenticita) – overenie originálnosti a platnosti správy a identity jej pôvodcovi. Najčastejšie sa na zaistenie tejto podmienky využívajú certifikáty. [4]
- Accountability (Sledovateľnosť) – identifikácia prístupu k informáciám a vysledovateľnosť bezpečnostných incidentov v prípade využitia forenznej analýzy. Väčšinou je táto požiadavka zaistená záznamom činnosti v systéme formou logu. [4]

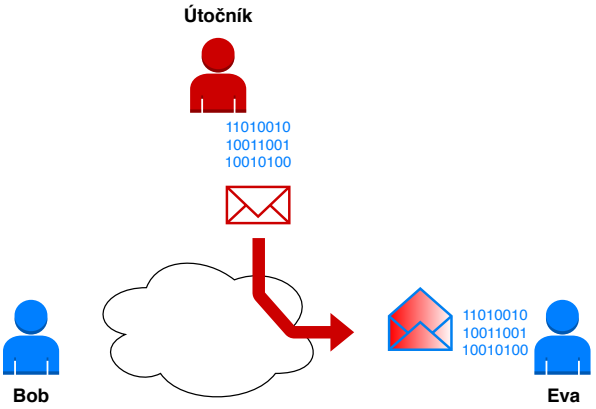
1.3 Pasívne a aktívne útoky

Útoky na bezpečnosť môžu byť rozdelené do dvoch skupín. Jednou skupinou je pasívny útok, kde nepozmeňuje útočník pôvodné dáta a nevplýva na príjemcu týchto dát. Druhou možnosťou je aktívny útok, pri ktorom sú buď pozmenené dáta doručené príjemcovi alebo je obeť nejakým spôsobom ovplyvňovaná, napríklad zasielaním falošných informácií. [2]

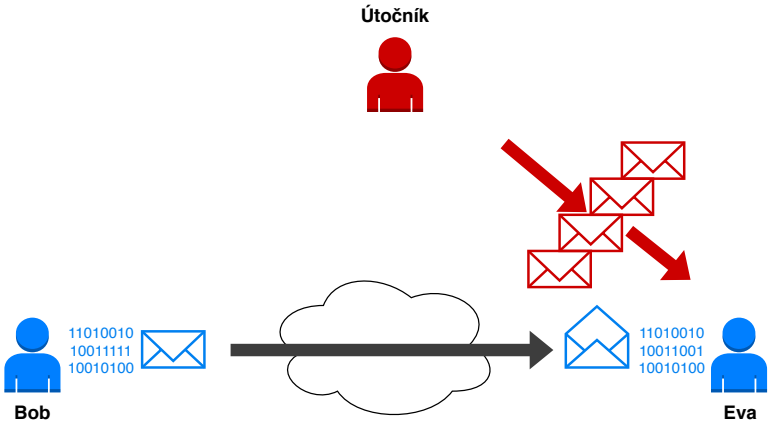


Obr. 1.3: Pasívny útok [4]

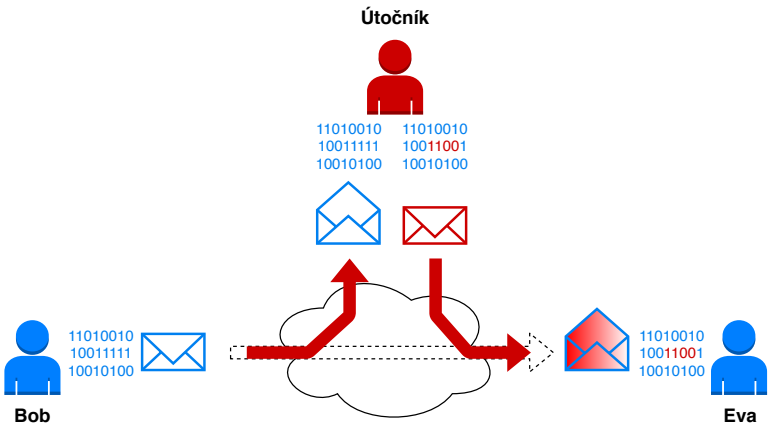
Pri pasívnom útoku, ktorý je znázornený na obrázku 1.3 ide útočníkovi prevažne o zachytenie prenášanej komunikácie a monitorovanie a analýzu prevádzky. Odposluch a zobrazenie obsahu dát je účinné hlavne pri nepoužití šifrovania správ medzi koncovými bodmi alebo aj pri použití slabých šifier, krátkych kľúčov a nedostatočne bezpečných hesiel. Monitorovanie prevádzky, respektíve analýza komunikácie je možná aj pri použití šifrovania, keďže každá komunikácia je charakteristická určitým vzorom. Pasívne útoky je nesmierne obtiažne detegovať nakoľko nemodifikujú dáta pri prenose. Najúčinnejšia obrana je použitie dostatočne silných šifier na zabezpečenie dát. Jeden z pasívnych útokov sa hojne využíva aj pri prevencii v *Intrusion Detection System – systém detekcie narušenia* (IDS) a *Intrusion Prevention System – systém prevencie prienikov* (IPS), kde bez analýzy prevádzky by nebolo možné zabezpečiť sieť. Pasívnymi útokmi sa nespôsobuje škoda na systéme alebo infraštruktúre, ale hrozba spočíva v narušení dôvernosti.



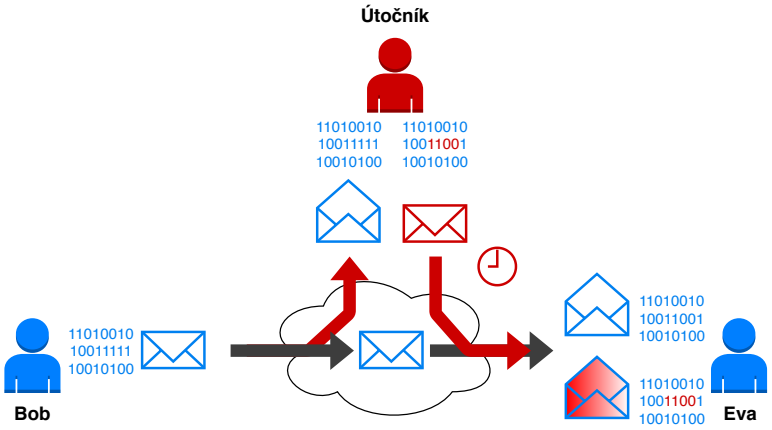
Obr. 1.4: Aktívny útok maškaráda [4]



Obr. 1.5: Aktívny útok DOS [4]



Obr. 1.6: Aktívny útok modifikácia správy [4]



Obr. 1.7: Aktívny útok prehratím [4]

Aktívne útoky sú sofistikovanejšie ako pasívne, modifikujú dáta alebo vytvárajú falošné, o ktorých prijímateľ predpokladá, že prišli od zdroja, s ktorým pôvodne komunikoval. Hrozby, ktoré môžu týmito útokmi nastať sú strata integrity, teda modifikácia dát a ohrozenie dostupnosti pričom vždy dochádza ku škode na systéme alebo infraštruktúre. Maškaráda je prvým z aktívnych útokov, kde ako je možné vidieť na obrázku 1.4, útočník vytvára falošnú správu, ktorú zasiela obeti a tá sa domnieva, že komunikuje s pôvodným zdrojom, v našom prípade Bobom. Príkladom aktívneho útoku je aj útok odoprenia služby 1.5, kde sa vytvárajú falošné dáta generované vysokou frekvenciou za účelom odstaviť systém alebo infraštruktúru, ktorá nezvláda spracovanie toľkých požiadaviek, keďže nebola na takúto záťaž dimenzovaná. Tretím aktívnym útokom 1.6 je modifikácia správy útočníkom pri prechode komunikačným kanálom, ktorý sa realizuje rôznymi technikami podvrhnutia zdroja alebo identity. Posledným útokom je útok prehratím 1.7, čo je útok veľmi podobný predchádzajúcemu, akurát obeť obdrží najprv pôvodnú nepozmenenú správu a následne po určitom čase aj modifikovanú správu od útočníka.

2 Bezpečnostný audit

Auditovanie je veľmi dôležitým prvkom správy informačných systémov a infraštruktúry, pretože umožňuje zaistiť bezpečnosť týchto informačných aktív porovnávaním s vytvorenými štandardmi, odporúčaniami a predpismi. Zaoberá sa otázkami čo a ako zabezpečiť, vyhodnocovaním a riadením rizík a následným dokazovaním, že náprava znížila riziko hrozby.

Auditovanie sa skladá z piatich pilierov [5]:

1. Posúdenie
2. Prevencia
3. Detekcia
4. Reakcia
5. Zotavenie

Pri posudzovaní si je potreba klásť otázky či sú prístupové práva dostatočne špecifikované, aká je pravdepodobnosť útoku na zraniteľnosť a podobne. Prevencia nespočíva iba v technológiách ako firewall prípadne IDS a IPS, ale aj v politikách, procesoch a povedomí o probléme. Detekcia a reakcia spolu úzko súvisia a je potrebné skrátiť dobu medzi týmito dvoma bodmi, bez dôkladnej detekcie nie je možné vykonať reakciu. Mnohé reakcie na detekciu problému sú už rôznymi technológiami implementované automatizovane. Posledný článkom je zotavenie, ktoré je dôležité pri službách vysokej dostupnosti. Výborným príkladom detekcie, reakcie a zotavenia z problému sú protokoly z rodiny *First Hop Redundancy Protocol* (FHRP).

Proces auditu pozostáva z niekoľkých fází: [5]

1. Plánovanie – stanovenie cieľov a predmetu auditu. Definuje sa rozsah, teda čo všetko je v pláne auditom pokryť.
2. Výskum – vytváranie auditného plánu na základe štandardov a odporúčaní a špeciálnych expertíz. Kontaktujú sa tiež dotknuté strany, ktoré nám môžu byť nápomocné pri plnení cieľov.
3. Zbieranie dát – vyžiadanie potrebných podkladov a dát na vykonanie auditu, zozbieranie dôkazov. V tejto fáze sa tiež vyberajú rôzne softvérové nástroje na vykonanie auditu a vytvorí sa checklist na základe auditného plánu a zozbieraných dôkazov.
4. Analýza dát – posúdenie všetkých dôkazových dát pomocou checklistu a softvéru na podporu auditu. Na základe nájdených nedostatkov sa vytvoria odporúčania, ktoré by mali znížiť riziká hrozieb.
5. Vytváranie správy – súpis nájdených nedostatkov, možných riešení na zníženie rizík do auditnej správy a prezentácia tejto správy dotknutým stranám.

6. Aplikácia opatrení – nasadenie a použitie protiopatrení prezentovaných alebo vyplývajúcich z auditnej správy. Následne sa môže vykonať monitorovanie a hlásenie o úspešnosti zmien.

Typy auditov podľa zistení, hĺbky a rozsahu auditu:

- Bezpečnostná kontrola – je najzákladnejšia forma analýzy bezpečnosti, na základe ktorej sa následne formujú ďalšie aktivity na zaistenie bezpečnosti. Do tejto kategórie spadajú automatizované nástroje na skenovanie zraniteľností a penetračné nástroje, ktoré generujú zoznam potenciálnych zraniteľností, ale je potrebné ďalšie podrobnejšie preskúmanie výsledkov a zistení a stanovenie, ako sa k ním zachovať. Patria sem nástroje ako napríklad Nmap, Nessus a podobne. Za bezpečnostnú kontrolu možno považovať preskúmanie politík alebo architektúry daného systému a infraštruktúry. Dá sa povedať, že ide o akýsi rýchly náhľad na bezpečnosť, ktorého výstupom je poznanie a identifikovanie problému.
- Hodnotenie bezpečnosti – je ďalším stupňom, pričom ide o podrobnejší pohľad na problém z profesionálnejšieho hľadiska. Kvalifikuje sa riziko k jednotlivým zisteniam a stanovuje sa relevantnosť a kritickosť týchto zistení na konkrétnu organizáciu a prípad použitia.
- Bezpečnostný audit – je štandardizovanou a najdôkladnejšou formou posúdenia bezpečnosti. Bezpečnosť sa porovnáva so štandardmi alebo benchmark-mi, v niektorých prípadoch aj s predpismi dohliadahúcich orgánov. Výsledkom je posúdenie, na koľko je organizácia alebo skúmaný objekt v zhode s porovnávaným štandardom. Typickým príkladom štandardov sú ISO27001 a COBIT.

2.1 Manažment rizík

Manažment rizík je proces pozostávajúci z analýzy rizík a riadenia rizík [3]. Dôležitým faktom je, že riziko nie je možné eliminovať, ale ho iba znížiť.

Pri analýze rizík zisťujeme, aké riziká existujú, ako medzi sebou súvisia a aké škody môžu spôsobiť. Analýza rizík môže byť vykonávaná kvalitatívne a kvantitatívne.

Štandard NIST SP 800-30 [6] definuje nasledujúce kroky pri analýze rizík:

1. Identifikácia informačných aktív a ich význam
2. Identifikácia hrozieb
3. Identifikácia zraniteľností
4. Analýza riadenia a kontroly
5. Zistenie pravdepodobnosti
6. Identifikovanie dopadu
7. Definovanie rizika ako súčinu pravdepodobnosti a dopadu
8. Odporúčanie na zavedenie riadenia a kontroly na zníženie rizika
9. Zdokumentovanie výsledkov

Riadenie rizík má za úlohu minimalizáciu potenciálnych škôd odhalených pri analýze rizík s ohľadom na vyváženie nákladov na riadenie rizika.

Prístupy k nájdenému riziku [2][3][5]:

- Vyhnutie sa riziku – je uplatnené ak prítomnosť a funkčnosť informačného aktíva nestojí za podstúpenie rizika, a teda toto aktívum vôbec nepoužijeme. Napríklad vypnutie menej bezpečných a nevyužívaných sieťových služieb.
- Zníženie – aplikovanie protiopatrenia na odstránenie hrozby alebo zraniteľnosti prípadne zníženie pravdepodobnosti rizika. Nikdy nie je však možné riziko eliminovať. Príkladom môže byť obmedzenie prístupu k sieťovému prvku.
- Akceptovanie – v prípade neexistujúceho protiopatrenia alebo veľmi nízkeho rizika. Častokrát ide o bezpečnostnú chybu softvéru v službe, ktorú využívame a nie je možné ju vypnúť ani aplikovať protiopatrenie.
- Presun – riziko je možné presunúť na inú organizáciu, napr. poistenie v prípade škody spôsobenej nedostatočným zabezpečením.
- Ignorácia – úplné vypustenie faktu, že dochádza k riziku, tento prístup sa považuje za iracionálny.

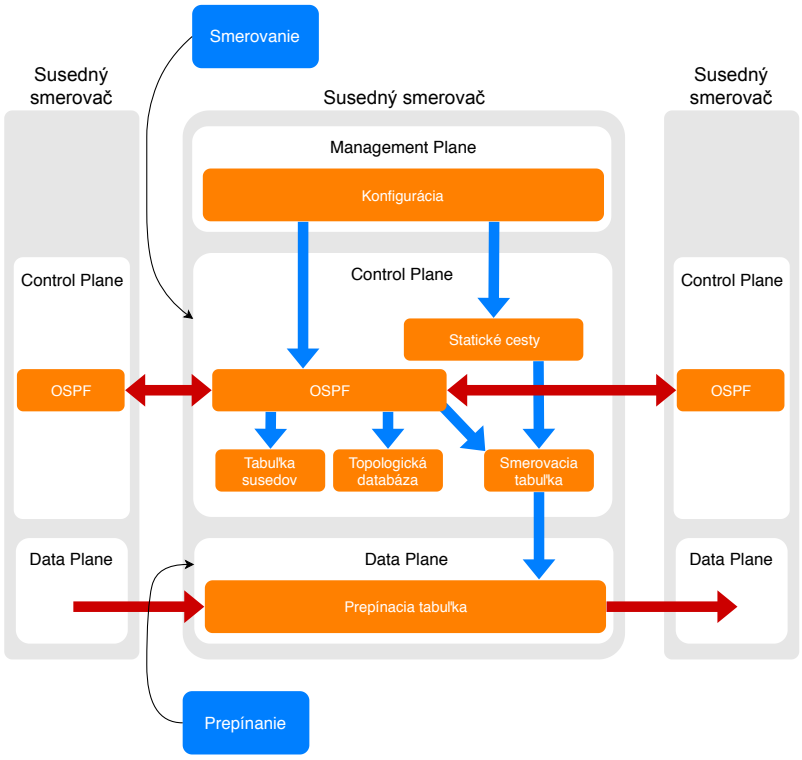
Na ohodnotenie rizika slúžia rôzne systémy hodnotenia, jedným z nich je *Common Vulnerability Scoring System* (CVSS), ktorý definuje riziká podľa definovaných metrík na základe dosiahnutého skóre do nasledujúcich tried:

- 0: No issue
- 0,1 – 3,9: Low
- 4,0 – 6,9: Medium
- 7,0 – 8,9: High
- 9,0 – 10,0: Critical

3 Prevádzka a bezpečnosť sietí

Sieťové prvky sú zodpovedné nielen za preposielanie dát medzi koncovými stanicami, ale aj za mnohé riadiace dáta medzi sebou, bez ktorých by sieť nebola funkčná. Preto sa jednotlivé protokoly a služby rozdeľujú troch rovín alebo úrovní, a to management, control a data plane. Tieto pojmy sa využívajú vo väčšej miere v softvérovo definovaných sieťach, no sú platné aj v klasickej koncepcii.

Úroveň management plane je zodpovedná za konfiguráciu zariadení a riadenie prístupu ku konfiguráciám. Typickými príkladmi protokolov pracujúcich na tejto úrovni sú *Simple Network Management Protocol* (SNMP), *Authentication Authorization Accounting* (AAA), Syslog, *Secure Shel* (SSH) a mnohé ďalšie [7]. Druhá úroveň control plane má na starosti prevažne smerovanie, teda kadiaľ budú pakety smerované a prenáša riadiace a signalizačné informácie pre protokoly ako napríklad, *Open Shortest Path First* (OSPF), Spanning tree, FHRP [7]. Poslednou úrovňou je data plane nazývaná často aj forwarding plane, ktorá prepína a pakety na daný port na základe rozhodnutie z control plane. Táto časť sieťových prvkov musí byť veľmi rýchla, aby zaistila nízku odozvu a dostatočne vysoké prenosové rýchlosti. Nižšie uvedený obrázok



Obr. 3.1: Rozdelenie úrovní v smerovači [8]

3.1 Hierarchia sietí

3.2 Riadenie a zneužitie prístup

AAA, username, accounts, enable psswd, ssh, ACL(data plane, je to data plane?) 92, 111, 112, bannery plus logovanie neuspesnych pristupov

3.3 Smerovacie protokoly

autentizacia, passive, ip source routing, urpf

3.4 Identifikácia zariadení, pravidiel a nastavení

host,domainname, acl remark, int description

3.5 Šifrovanie hesiel

3.6 Logovanie

syslog, snmp nastavenie oboch, plus co logovat, teda accouting a logovanie deny pravidiel, 93

3.7 Synchronizácia času

ntp + amplifikacne utoky

3.8 Záloha a zabezpečenie konfigurácií

archive, tftp, scp, delete protection, logovanie zmien, mozno netreba, ak je AAA accounting

3.9 Správanie pri vysokom zaťažení

68-71, storm control

3.10 Monitorovanie výkonu siete

SPAN NETFLOW

3.11 Problémy vrstvy L2

access, max, hopping, double tagging, blackhole, default access a trunk, dtp, spanning tree, dot1x, vtp

3.12 First Hop Security

130 - 138 140 144-148 aj mac spoof a mac floof, teda spanning tree prikazy!!! http://isp-servis.com/?p=191

3.13 First Hop Redundancy Protocols

3.14 Tunely

3.15 Mapovanie siete a objavovanie zariadení

proxy arp, 88-91, lldp, cdp, 139

3.16 Nepoužívané a nebezpečné služby

3.17 Ostatné

source interfaces loopback shutdown

4 Návrh

TODO
Excel tabuľka s redukciou stĺpcov(checklist) - možno do príloh, ak to bude rozsiahle
Checklist ako vznikal a ako boli vypĺňaná polia severity a facility
Rozdelenie príkazov
Rozdelenie zariadení podľa vrstvy - popísať
Stromová štruktúra a koncept fungovania
Možno fungovanie cez nejaký UML diagram (sekvenčný?)
Prečo konfigurák YAML, výhody a porovnanie s JSON a XML
Niečo o Pythone a prečo bol vybraný (možno do implementácie)
Popísať konfiguračné súbory device.yaml module.yaml (možno do implementácie)

5 Implementácia

TODO
Rozdelenie zariadení a automatické vypĺňanie štruktúr YAML súborov
Matchovanie cez regexy, teória o REGEX (možno do teórie)

Záver

Zhrnutie práce.

Literatúra

[1] MILKOVICH, Devon. 13 Alarming Cyber Security Facts and Stats. In: *Cybint* [online]. 3.12.2018 [cit. 2019-11-08]. Dostupné z: https://www.cybintsolutions.com/cyber-security-facts-stats/

[2] VYNCKE, Eric a Christopher PAGGEN. *LAN switch security: What hackers know about your switches*. Indianapolis, IN: Cisco Press, 2008. ISBN :978-1-58705-256-9.

[3] MCMILLAN, Troy. *CCNA security study guide: exam 210-260*. Indianapolis, Indiana: Sybex, a Wiley Brand, 2018. ISBN 978-111-9409-939.

[4] STALLINGS, William. *Network security essentials: applications and standards*. 4th ed. Boston: Prentice Hall, 2011. ISBN 978-0-13-610805-4.

[5] JACKSON, Chris. *Network security auditing*. Indianapolis, IN: Cisco Press, 2010. Cisco Press networking technology series. ISBN 978-1-58705-352-8.

[6] Guide for Conducting Risk Assessments: NIST Special Publication 800-30. In: *NIST* [online]. 2012 [cit. 2019-11-08]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[7] SINGH, Shashank. Cisco Guide to Harden Cisco IOS Devices. In: *Cisco* [online]. 2018 [cit. 2019-11-02]. Dostupné z: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

[8] PEPELNJAK, Ivan. Management, Control and Data Planes in Network Devices and Systems. In: *IpSpace* [online]. 2013 [cit. 2019-11-17]. Dostupné z: https://blog.ipspace.net/2013/08/management-control-and-data-planes-in.html

[9] ALSADEH, Ahmad. Augmented SEND: Aligning Security, Privacy, and Usability. In: *RIPE NCC* [online]. 12.5.2015 [cit. 2019-11-02]. Dostupné z: https://ripe70.ripe.net/presentations/67-RIPE70-SEND.pdf

[10] PODERMAŃSKI, Tomáš a Matěj GRÉGR. Bezpečné IPv6: zkrocení zlých směrovačů. In: *ROOT.CZ* [online]. 12.2.2015 [cit. 2019-11-02]. Dostupné z: https://www.root.cz/clanky/bezpecne-ipv6-zkroceni-zlych-smerovacu/

[11] KHANDELWAL, Manjul. OSPF Security: Attacks and Defenses. In: *SANOG* [online]. 2016 [cit. 2019-11-04]. Dostupné z: https://www.sanog.org/resources/sanog28/SANOG28-Tutorial_OSPF-Security-Attacks-and-Defences-Manjul.pdf

[12] PODERMAŃSKI, Tomáš a Matěj GRÉGR. Bezpečné IPv6: když dojde keš — obrana. In: *ROOT.CZ* [online]. 19.3.2015 [cit. 2019-11-02]. Dostupné z: https://www.root.cz/clanky/bezpecne-ipv6-kdyz-dojde-kes-obrana/

[13] PODERMAŃSKI, Tomáš a Matěj GRÉGR. Bezpečné IPv6: když dojde keš. In: *ROOT.CZ* [online]. 12.3.2015 [cit. 2019-11-02]. Dostupné z: https://www.root.cz/clanky/bezpecne-ipv6-kdyz-dojde-kes/

[14] PODERMAŃSKI, Tomáš a Matěj GRÉGR. Bezpečné IPv6: trable s multicastem. In: *ROOT.CZ* [online]. 5.3.2015 [cit. 2019-11-02]. Dostupné z: https://www.root.cz/clanky/bezpecne-ipv6-trable-s-multicastem/

[15] GRÉGR, Matěj a Tomáš PODERMAŃSKI. Bezpečné IPv6: vícehlavý útočník. In: *ROOT.CZ* [online]. 26.2.2015 [cit. 2019-11-02]. Dostupné z: https://www.root.cz/clanky/bezpecne-ipv6-vicehlavy-utocnik/

[16] PODERMAŃSKI, Tomáš a Matěj GRÉGR. Bezpečné IPv6: trable s hlavičkami. In: *ROOT.CZ* [online]. 19.2.2015 [cit. 2019-11-02]. Dostupné z: https://www.root.cz/clanky/bezpecne-ipv6-trable-s-hlavickami/

[17] GRÉGR, Matěj a Tomáš PODERMAŃSKI. Bezpečné IPv6 : směrovač se hlásí. In: *ROOT.CZ* [online]. 5.2.2015 [cit. 2019-11-02]. Dostupné z: https://www.root.cz/clanky/bezpecne-ipv6-smerovac-se-hlasi/

[18] IPv6 First-Hop Security Configuration Guide. In: *Cisco* [online]. San Jose [cit. 2019-11-02]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-1sg/ip6f-15-1sg-book.pdf

[19] BOUŠKA, Petr. *Cisco IOS 12 - IEEE 802.1x a pokročilejší funkce* [online]. In: . 2007 [cit. 2019-11-02]. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-ios-12-ieee-802-1x-a-pokrocilejsi-funkce/

[20] MOLENAAR, René. Cisco IOS features that you should disable or restrict. In: *NetworkLessons.com* [online]. [cit. 2019-11-02]. Dostupné z: https://networklessons.com/uncategorized/cisco-ios-features-that-you-should-disable-or-restrict

[21] BOUŠKA, Petr. Cisco IOS 23 - Autentizace uživatele na switchi vůči Active Directory. In: *SAMURAJ-cz* [online]. 2009 [cit. 2019-11-02]. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-ios-23-autentizace-uzivatele-na-switchi-vuci-active-directory/

[22] BARKER, Elaine a Allen ROGINSKY. Transitioning the Use of Cryptographic Algorithms and Key Lengths. In: *NIST* [online]. 2019 [cit. 2019-11-02]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf

[23] VYNCKE, Erik. ND on wireless links and/or with sleeping nodes. In: *IETF* [online]. [cit. 2019-11-02]. Dostupné z: https://www.ietf.org/proceedings/89/slides/slides-89-v6ops-3.pdf

[24] CIS Cisco IOS 15 Benchmark. In: *Center For Internet Security* [online]. 2015 [cit. 2019-11-02]. Dostupné z: https://www.cisecurity.org/benchmark/cisco/

[25] GRAESSER, Dana. Cisco Router Hardening Step-by-Step. In: *SANS Institute* [online]. 2001 [cit. 2019-11-02]. Dostupné z: https://www.sans.org/reading-room/whitepapers/firewalls/paper/794

[26] PILIHANTO, Atik. A Complete Guide on IPv6 Attack and Defense. In: *SANS Institute* [online]. SANS Institute, 2012 [cit. 2019-11-02]. Dostupné z: https://www.sans.org/reading-room/whitepapers/detection/paper/33904

[27] REY, Enno, Antonios ATLASIS a Jayson SALAZAR. MLD Considered Harmful. In: *RIPE NCC* [online]. 2016 [cit. 2019-11-02]. Dostupné z: https://ripe72.ripe.net/presentations/74-ERNW_RIPE72_MLD_Considered_Harmful_v1_light_web.pdf

[28] VYNCKE, Erik. IPv6 First Hop Security: the IPv6 version of DHCP snooping and dynamic ARP inspection. In: *Slidde Share* [online]. 2012 [cit. 2019-11-02]. Dostupné z: https://www.slideshare.net/IKTNorge/eric-vyncke-layer2-security-ipv6-norway

[29] IPv6 First-Hop Security Configuration Guide. In: *Cisco* [online]. 2012 [cit. 2019-11-02]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-s/ip6f-15-s-book/ip6-snooping.html

[30] GREGR, Matej, Petr MATOUSEK, Miroslav SVEDA a Tomas PODERMANSKI. Practical IPv6 monitoring-challenges and techniques. In: *12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011) and Workshops*. IEEE, 2011, 2011, s. 650-653. DOI: 10.1109/INM.2011.5990647. ISBN 978-1-4244-9219-0. Dostupné také z: http://ieeexplore.ieee.org/document/5990647/

[31] PODERMAŃSKI, Tomáš a Matějj GRÉGR. *Deploying IPv6 - practical problems from the campus perspective* [online]. In: . [cit. 2019-11-02].

[32] MARTIN, Tim. IPv6 Sys Admin Style. In: *SlideShare* [online]. 2016 [cit. 2019-11-02]. Dostupné z: https://www.slideshare.net/tjmartin2020/ipv6-sysadmins-63071235

[33] Cisco SAFE Reference Guide. In: *CIsco* [online]. San Jose, CA, 8 Júl 2018 [cit. 2019-11-02]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_

[34] SAFE Overview Guide: Threats, Capabilities, and the Security Reference Architecture. In: *Cisco* [online]. Január 2018 [cit. 2019-11-02]. Dostupné z: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-overview-guide.pdf

[35] AKIN, Thomas. *Hardening Cisco routers*. Sebastopol: O'Reilly, 2002. ISBN 05-960-0166-5.

[36] HUCABY, Dave, Steve MCQUERRY, Andrew WHITAKER a Dave HUCABY. *Cisco router configuration handbook*. 2nd ed. Indianapolis, IN: Cisco Press, 2010. ISBN 978-1-58714-116-4.

[37] SATRAPA, Pavel. *IPv6: internetový protokol verze 6*. 4. aktualizované a rozšířené vydání. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-808-8168-430.

Zoznam symbolov, veličín a skratiek

CIA	confidentiality, integrity, availability – dôvernosť, integrita, dostupnosť
DDoS	Distributed Denial of Service – distribuované odoprenie služby
DoS	Denial of Service – odoprenie služby
ACL	Access Control List – zoznam pre riadenie prístupu
CVSS	Common Vulnerability Scoring System
IDS	Intrusion Detection System – systém detekcie narušenia
IPS	Intrusion Prevention System – systém prevencie prienikov
FHRP	First Hop Redundancy Protocol
SNMP	Simple Network Management Protocol
AAA	Authentication Authorization Accounting
SSH	Secure Shel
OSPF	Open Shortest Path First

Zoznam príloh

A Zdrojové súbory

A.1 Konfiguračné súbory

B Checklist